משפטי סילו

תוצאות מסילו 1

1) נניח $p^n \mid |G|$ (p ראשוני, $n\in\mathbb{N}$). אזי לכל $0\le k\le n$, קיימת תת"ח מגודל p^k.

הסבר: נניח $|G|=p^t m$ כאשר $(p,m)=1$.
בהכרח ש- $n\le t$.
לפי סילו 1 יש תת"ח p-סילו P כך ש- $|P|=p^t$
ממשפט על חבורות p לכל $0\le k$ קיימת תת"ח $P\ge H$
$|H|=p^k$, ולכן $G\ge H$.

ב) משפט קושי:
תהי G חבורה סופית ו $p \mid |G|$ (p ראשוני). אזי יש $a\in G$ שמסדרו $p=o(a)$.

משפט סילו 2

תהי חבורה G סופית $|G|=p^n m$, p ראשוני $(p,m)=1$. אזי
א) כל תת"ח p $H\le G$ מוכלת בתת"ח p סילו.
ב) כל תת"ח p סילו צמודות.

הוכחה

א) נניח $|H|=p^k$, $k\ge 1$, ונעיר שאם $P\in Syl_p(G)$, אז
לכל $g\in G$: $gPg^{-1}\in Syl_p(G)$ (כי הצמדה אוטומורפיזם).
לכן יש פעולת הצמדה $G\times Syl_p(G)\to Syl_p(G)$ $\quad (g,P)\mapsto gPg^{-1}$
ומסילו 1 $Syl_p(G)\neq\emptyset$, $P\in Syl_p(G)$, ומוגדרת פעולה
$G\times G/P\to G/P$
$(g,tP)\mapsto (gt)P$ ויש מסילו 1.
ובפרט שמוגדרת פעולת הצמצום $H\times G/P\to P$
אבל הפעם אין הכרח שיהיה מסילו 1,
$|H|=p^k$ ולכן נשתמש בטענה לפיה לכל $H\times X\to X$ עבור H ק-ח
$|F|\equiv |X| \mod p$, במקרה זה $|F|\equiv |G/P| \mod p$
$|F|\equiv m \mod p$
$(m,p)=1 \Rightarrow m\not\equiv 0 \mod p \Rightarrow |F|\not\equiv 0 \mod p$
ולכן יש נקודת שבת $x := gP\in G/P$

נקבל $\forall h\in H \quad h(gP)=gP$

$$g^{-1}hgP=P$$

$$g^{-1}hg\in P$$

$\exists g\in G;\ \forall h\in H: \quad h\in gPg^{-1}\in Syl_p(G)$

$$H\leq gPg^{-1}$$

בד מוכיח (k) ע״פ (Q) אם $H:=P_1\in Syl_p(G)$

$$P_1\leq gPg^{-1}$$

ומכן אחד יש רק אוקרום ולכן $P_1=gPg^{-1}=P_1$

משפט סילו 3

תהי G כנ״ל, מ״מ $|G|=p^n m$ $(p,m)=1$

א $n_p=[G:N(P)]$ מספר תת״ח p סילו.

ב $n_p\equiv 1 \mod p$

ג $n_p|m$

הוכחה

א) לפי סילו 2 ופעולה $G\times Syl_p(G)\to Syl_p(G)$ הקודמת ע״י הצמדות יש מסלול אחד!

לפי נוסחה של גודל המסלול $|[x]|=[G:G_x]$

נציב ונקבל $n_p=|[P]|=[G:G_P]=[G:N(P)]$

ב) נקח את צמצום הפעולה $P\times Syl_p(G)\to Syl_p(G)$ ע״י הצמדות

לפי משפט א׳ נק׳ שבת

$$n_p=|Syl_p(G)|\equiv|F| \mod p$$

נוכיח $|F|=1$. $P\in F$ ולכן $|F|\geq 1$.

נקח נניח $Q\in F$, צ״ל $Q=P$.

$$\Downarrow$$

$Q\leq N(P)$, $P\leq N(Q)$ $\Leftarrow$ $\forall g\in P \quad gQg^{-1}=Q$

ואז שני תת״ח p סילו של $N(Q)$, לכן לפי סילו 2 P,Q צמודות ב- $N(Q)$: $\exists t\in N(Q): P=tQt^{-1}=Q$

לכן $|F|=1$ כנדרש.

$$m=[G:P]=[G:N(P)][N(P):P]=n_p[N(P):P]$$

ולכן $n_p \mid m$

הערה

$$[N(P):P]=\frac{m}{n_p}$$

משפט ברנסייד

לכל פעולה $G\times X\to X$ של חבורה סופית G על קבוצה סופית X, מס' המסלולים יהיה

$$k=\frac{1}{|G|}\sum_{g\in G}|X_g|$$

הוכחה:

שלב א נוכיח ש: $\sum_{x\in X}|G_x|=\sum_{g\in G}|X_g|$

נגדיר פונקציה $F: G\times X\to\{0,1\}$

$$F(g,x)=\begin{cases}1 & g*x=x\\ 0 & else\end{cases}$$

ונגדיר טבלה של נקודות שבת.

F	x_1	x_2	$\dots$	x_n
$e=g_1$	1	1		1
g_2	0	1	$\dots$	0
$\vdots$				
g_n				

למשל

ולפי שורות
$\|$
ולפי עמודות $\Rightarrow$ $\sum_{g\in G}|X_g|=\sum_{x\in X}|G_x|$ כנדרש

שלב ב: נוכיח נוסחת ברנסייד, שקול להוכיח

$$\sum_{x\in X}|G_x|=k|G|$$

$$\sum_{x\in X}|G_x|=\sum_{i=1}^{k}\sum_{y\in[x_i]}|G_y|=\sum_{i=1}^{k}\sum_{y\in[x_i]}\frac{|G|}{|[y]|}=\sum_{i=1}^{k}\frac{|G|}{|[x_i]|}|[x_i]|=k|G|$$

יהיו $x_1,\dots,x_k$ נציגים של מסלולים

כנדרש!

הערות נוספות על חבורות פתירות

הגדרה

אם G חבורה ו- $a,b\in G$ הקומוטטור יהיה
$$[a,b]:=aba^{-1}b^{-1}$$

תכונות של קומוטטורים:

* $[a,b]=e \iff ab=ba$
* $[a,b]^{-1}=[b,a]$
* $g[a,b]g^{-1}=[gag^{-1},gbg^{-1}]$
* $G':=\langle [a,b] \mid a,b\in G\rangle \trianglelefteq G$. $G'=\{e\}$ אמ"מ G אבלית.
* G/G' אבלית.
* הכללה: עבור $N\trianglelefteq G$, אז G/N אבלית $\iff$ $G'\subseteq N$.
* G פתירה $\iff$ קיים $n\in\mathbb{N}$ עבורו $G^{(n)}=\{e\}$, כאשר $G^{(n)}=(G^{(n-1)})'$

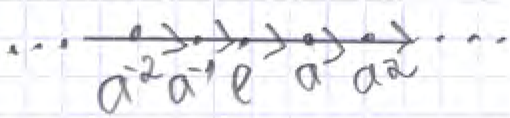
<u>חבורה חופשית (קבוצת יוצרים ויחסים)</u>

דוגמאות

1) עבור $G=\langle a\rangle$ צקלית:

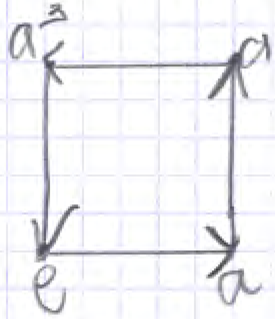
אינסופית. $G=\langle a\mid\emptyset\rangle$

אין יחסים



סופית עם n איברים $G=\langle a\mid a^n=e\rangle$

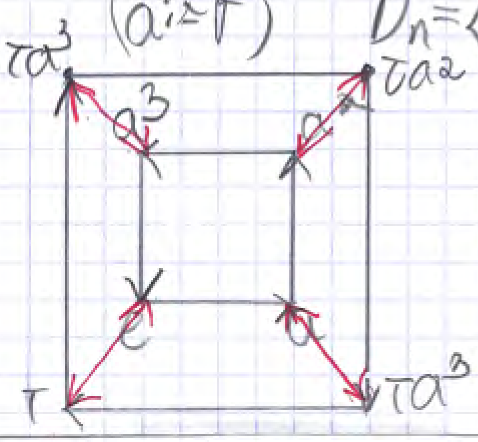
עבור $n=4$ הגרף יהיה



2) עבור $D_n=\left\langle \sigma,\tau \,\middle|\, \begin{matrix}\sigma^n=e\\ \tau^2=e\\ \sigma\tau=\tau\sigma^{-1}\end{matrix}\right\rangle$

עבור $n=4$

$(a:=\sigma)$



בנייה של גרף קיילי של חבורה $G=\langle \underset{\text{יוצרים}}{S} \mid \underset{\text{יחסים}}{R} \rangle$:

1) הקודקודים הם איברים של G.

2) לכל $s\in S$ יהיה צבע.

3) $x \xrightarrow{a} ax$

הגדרה

חבורה חופשית היא חבורה מהצורה $\langle S \mid \emptyset\rangle$ או $\langle S \mid \text{יחסים טריוויאלים}\rangle$

ונסמן $F(S)$

דוגמא

א) $F(a)=\langle a \mid \emptyset\rangle \simeq \mathbb{Z}$

ב) $F(a,b):=\langle a,b \mid \emptyset\rangle$ מילים מהאותיות $\{a,b\}$.

תכונות

1) לכל חבורה $G=\langle S \mid R\rangle$ קיים אפימורפיזם טבעי

$$F(S) \longrightarrow G$$

$$s_1^{r_1}s_2^{r_2}\cdots s_t^{r_t} \longmapsto s_1^{r_1}\cdot s_2^{r_2}\cdots s_t^{r_t}$$

2) $G_1=\langle S \mid R_1\rangle$, $G_2=\langle S \mid R_2\rangle$, $R_1\subseteq R_2$. אזי קיים אפימורפיזם

$$G_1 \longrightarrow G_2$$

3) חבורה חופשית אבלית

$$A(S)=\langle S \mid \forall x,y\in S: xy=yx\rangle$$

ולכל $G=\langle S \mid R\rangle$ אבלית קיים אפימורפיזם

$$f: A(S) \to G$$

דוגמא

$$\mathbb{Z}^2 \simeq A(a,b)=\langle a,b \mid ab=ba\rangle$$

$$\mathbb{Z}^n \simeq A(a_1,\dots,a_n)$$

תרגיל

הוכח שכל חבורה אבלית סופית $\simeq \mathbb{Z}^n/H$.

פתרון

$\langle a_1,\dots,a_n \mid R\rangle$ אבלית לכן $a_i+a_j=a_j+a_i$. ומהמשפט לעיל

ראשון: $\mathbb{Z}^n \xrightarrow{f} G$ אפי' ע"י $\sum_{i=1}^{n} c_ie_i=(c_1,\dots,c_n)\mapsto \sum_{i=1}^{n} c_ia_i$